

# MAGNUS EMBEDDING AND ALGORITHMIC PROPERTIES OF GROUPS $F/N^{(d)}$

FUNDA GUL, MAHMOOD SOHRABI, AND ALEXANDER USHAKOV

**ABSTRACT.** In this paper we further study properties of Magnus embedding, give a precise reducibility diagram for Dehn problems in groups of the form  $F/N^{(d)}$ , and provide a detailed answer to Problem 12.98 in Kurovka notebook. We also show that most of the reductions are polynomial time reductions and can be used in practical computation.

**Keywords.** Magnus embedding, word problem, power problem, conjugacy problem, free solvable groups.

**2010 Mathematics Subject Classification.** 20F19, 20F10, 20F65, 03D15.

## 1. INTRODUCTION

Let  $F = F(X)$  be the free group on generators  $X$ ,  $N$  a normal subgroup of  $F$ ,  $N'$  the derived subgroup of  $N$ , and  $N^{(d)}$  the  $d$ th derived subgroup of  $N$ . The Magnus embedding is the main tool to study groups of the form  $F/N'$ . It was introduced in [7] by W. Magnus who showed that the elements of  $F/N'$  can be encoded by  $2 \times 2$  matrices:

$$M(X; N) = \left\{ \begin{pmatrix} g & \pi \\ 0 & 1 \end{pmatrix} \mid g \in F/N, \pi \in \mathcal{F}_\Gamma \right\},$$

where  $\mathcal{F}_\Gamma$  is a free module over the group ring  $\mathbb{Z}F/N$ . In this paper we study algorithmic properties of Magnus embedding and decidability of the following problems for groups of the form  $F/N^{(d)}$ .

**WP( $G$ ), word problem in  $G$ .** Given a word  $w$  in the generators of  $G$  decide if  $w = 1$  in  $G$ , or not.

**CP( $G$ ), conjugacy problem in  $G$ .** Given words  $u, v$  in the generators of  $G$  decide if  $u \sim v$  in  $G$ , or not.

**PP( $G$ ), power problem in  $G$ .** Given words  $u, v$  in the generators of  $G$  decide if  $v = u^k$  in  $G$  for some  $k \in \mathbb{Z}$ , or not.

The Magnus embedding proved to be especially robust in the study of free solvable groups. Indeed, free solvable group naturally appear in the context because

$$F/F^{(d)} = F/(F^{(d-1)})'$$

is the free solvable group of rank  $n$  and degree  $d$ . It immediately follows from the work of Magnus that decidability of the word problem in  $F/N$  implies decidability of the word problem in  $F/N'$ . The conjugacy problem in groups of the type  $F/N'$  was first approached by J. Matthews in [8] who proved that:

---

*Date:* January 7, 2015.

The third author has been partially supported by NSA Mathematical Sciences Program grant number H98230-14-1-0128.

- (a)  $u, v \in F/N'$  are conjugate (for free abelian  $F/N$ ) if and only if their images under Magnus embedding are conjugate in  $M(X; N)$ ;
- (b) conjugacy problem in  $M(X; N)$  is decidable if and only if conjugacy problem in  $F/N$  is decidable and power problem in  $F/N$  is decidable.

These two facts imply that free metabelian groups have decidable conjugacy problem. Later Remeslennikov and Sokolov in [15] extended (a) to any torsion free group  $F/N$ , showed that the power problem is decidable in free solvable groups, and deduced that free solvable groups have decidable conjugacy problem. Finally, C. Gupta in [4] proved that (a) holds for groups with torsion as well and hence decidability of the conjugacy and power problems in  $F/N$  implies decidability of the conjugacy problem in  $F/N'$ . We use the following notation for reducibility of decision problems in the sequel:

$$\begin{cases} \mathbf{CP}(F/N) \\ \mathbf{PP}(F/N) \end{cases} \Rightarrow \mathbf{CP}(F/N').$$

In the light of these results, V. Shpilrain raised the following questions in [9, Problem 12.98]. Is it correct that:

- (a)  $\mathbf{WP}(F/N)$  is decidable if and only if  $\mathbf{WP}(F/N')$  is decidable.
- (b)  $\mathbf{CP}(F/N)$  is decidable if and only if  $\mathbf{CP}(F/N')$  is decidable.
- (c)  $\mathbf{WP}(F/N')$  is decidable if and only if  $\mathbf{CP}(F/N')$  is decidable.

It was shown by Anokhin in [1] that only 12.98(a) has an affirmative answer. He constructed a group  $F/N$  such that  $\mathbf{CP}(F/N)$  is decidable and  $\mathbf{CP}(F/N')$  is undecidable. Such a group is clearly a counterexample to both 12.98(b) and 12.98(c).

We also would like to mention several results related to practical computations in free solvable groups in which the Magnus embedding plays a crucial role. S. Vassileva showed in [19] that the power problem in free solvable groups can be solved in  $O(rd(|u| + |v|)^6)$  time and used that result to show that the Matthews-Remeslennikov-Sokolov approach can be transformed into a polynomial time  $O(rd(|u| + |v|)^8)$  algorithm for the conjugacy problem. In [18] those complexity bounds were further improved and randomized algorithms were developed. Another generalization was done by Lysenok and Ushakov in [6]. It was shown that the Diophantine problem for spherical quadratic equations, i.e., equations of the form:

$$z_1^{-1}c_1z_1 \dots z_k^{-1}c_kz_k = 1,$$

in free metabelian groups is decidable. Recall that for every  $n \geq 2$  the Diophantine problem in free metabelian groups is undecidable (see [16]). Recently Vassileva proved in [20] that the Magnus embedding is a quasi-isometry.

**1.1. Our contribution.** Here we shortly outline the main results of the paper (somewhat simplifying the statements). Let  $F$  be a free group of rank at least 2 and  $N$  a recursively enumerable normal subgroup of  $F$ .

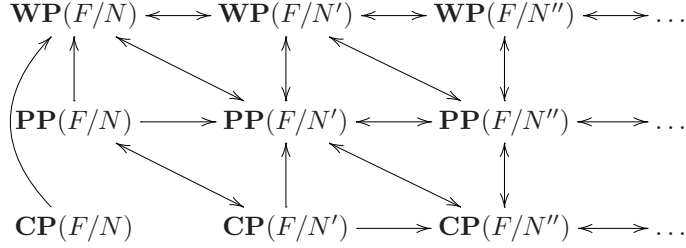
**Theorem 6.10.**  $\mathbf{WP}(F/N) \Rightarrow \mathbf{PP}(F/N')$ .

**Theorem 6.13.**  $\mathbf{PP}(F/N) \Rightarrow \mathbf{CP}(F/N')$ .

**Theorem 6.15.**  $\mathbf{PP}(F/N) \Leftarrow \mathbf{CP}(F/N')$ .

**Theorem 6.17.**  $\mathbf{CP}(F/N) \not\Rightarrow \mathbf{CP}(F/N')$ .

Our results give the following reducibility diagram for the decision problems in groups of the form  $F/N^{(d)}$ :



In particular, the following theorem holds.

**Corollary 6.16.** For every recursively enumerable  $N \leq F$  the following holds.

- (a)  $\mathbf{PP}(F/N') \Leftrightarrow \mathbf{PP}(F/N'')$ .
- (b)  $\mathbf{CP}(F/N'') \Leftrightarrow \mathbf{CP}(F/N''')$ .
- (c)  $\mathbf{WP}(F/N'') \Leftrightarrow \mathbf{PP}(F/N'') \Leftrightarrow \mathbf{CP}(F/N'')$ .

□

Furthermore, most of the reductions are polynomial time computable. Denote by  $\mathbf{P}$  the class of decision problems decidable in polynomial time.

**Theorem.** Suppose that  $\mathbf{WP}(F/N) \in \mathbf{P}$ . Then the problems  $\mathbf{WP}(F/N^{(d)})$ ,  $\mathbf{PP}(F/N^{(d)})$ , and  $\mathbf{CP}(F/N^{(d)})$  are in  $\mathbf{P}$  for every  $d \geq 2$ . Moreover, each of those problems has a unique polynomial bound that does not depend on  $d$ .

□

Finally, in Section 6.5 we consider two combinatorial problems for groups  $F/N'$ : subset sum problem  $\mathbf{SSP}(F/N')$  and acyclic graph problem  $\mathbf{AGP}(F/N')$ . The main results of that sections are:

**Theorem 6.20.**  $\mathbf{SSP}(F/N') \in \mathbf{P}$  if and only if  $\mathbf{WP}(F/N) \in \mathbf{P}$  and either  $N = \{1\}$  or  $[F : N] < \infty$ .

□

**Theorem 6.18.** If  $\mathbf{WP}(F/N) \in \mathbf{P}$ ,  $N \neq \{1\}$ , and  $[F : N] = \infty$ , then  $\mathbf{SSP}(F/N')$  and  $\mathbf{AGP}(F/N')$  are  $\mathbf{NP}$ -complete.

□

**Corollary 6.21.**  $\mathbf{AGP}(F/N') \in \mathbf{P}$  if and only if  $\mathbf{WP}(F/N) \in \mathbf{P}$  and either  $N = \{1\}$  or  $[F : N] < \infty$ .

□

## 2. PRELIMINARIES: $X$ -DIGRAPHS

Let  $X$  be a set (called an *alphabet*) and  $F = F(X)$  the free group on  $X$ . By  $X^-$  we denote the set of formal inverses of elements in  $X$  and put  $X^\pm = X \cup X^-$ . An  $X$ -labeled directed graph  $\Gamma$  (or an  $X$ -digraph) is a pair of sets  $(V, E)$  where the set  $V$  is called the *vertex set* and the set  $E \subseteq V \times V \times X^\pm$  is called the *edge set*. An element  $e = (v_1, v_2, x) \in E$  designates an edge with the *origin*  $v_1$  (also denoted by  $\alpha(e)$ ), the *terminus*  $v_2$  (also denoted by  $\omega(e)$ ), labeled with  $x$  (also denoted by  $\mu(e)$ ). We often use notation  $v_1 \xrightarrow{x} v_2$  to denote the edge  $(v_1, v_2, x)$ . A *path* in  $\Gamma$  is a sequence of edges  $p = e_1, \dots, e_k$  satisfying  $\omega(e_i) = \alpha(e_{i+1})$  for every  $i = 1, \dots, k-1$ . The *origin*  $\alpha(p)$  of  $p$  is the vertex  $\alpha(e_1)$ , the *terminus*  $\omega(p)$  is the vertex  $\omega(e_k)$ , and the *label*  $\mu(p)$  of  $p$  is the word  $\mu(e_1) \dots \mu(e_k)$ . We say that an  $X$ -digraph  $\Gamma$  is:

- *rooted* if it has a special vertex, called the root;
- *folded* (or deterministic) if for every  $v \in V$  and  $x \in X$  there exists at most one edge with the origin  $v$  labeled with  $x$ ;

- *X-complete* (or simply complete) if for every  $v_1 \in V$  and  $x \in X^\pm$  there exists an edge  $v_1 \xrightarrow{x} v_2$ ;
- *inverse* if with every edge  $e = g_1 \xrightarrow{x} g_2$  the graph  $\Gamma$  also contains the *inverse edge*  $g_2 \xrightarrow{x^{-1}} g_1$ , denoted by  $e^{-1}$ .

All  $X$ -digraphs in this paper are connected. A *morphism* of two rooted  $X$ -digraphs is a graph morphism which maps the root to the root and preserves labels. For more information on  $X$ -digraphs we refer to [17, 5].

**Example 2.1.** Let  $F = F(X)$  and  $H \leq F$ . The *Schreier graph* of the subgroup  $H$ , denoted by  $\mathbf{Sch}(X; H)$ , is an  $X$ -digraph  $(V, E)$ , where  $V$  is the set of right cosets

$$V = \{Hg \mid g \in F\}$$

and

$$E = \{Hg \xrightarrow{x} Hgx \mid g \in F, x \in X^\pm\}.$$

By definition,  $\mathbf{Sch}(X; H)$  is a folded complete inverse  $X$ -digraph. We always assume that  $H$  is the root of  $\mathbf{Sch}(X; H)$ . A special case of the Schreier graph is when  $H \trianglelefteq F$ , called a *Cayley graph* of the group  $F/H$  denoted by  $\mathbf{Cay}(X; H)$ .  $\square$

Let  $\Gamma = (V, E)$  be an inverse  $X$ -digraph. The set of edges  $E$  can be split into a disjoint union  $E = E^+ \sqcup E^-$ , where

$$E^+ = \{e \in E \mid \mu(e) \in X\}$$

is called the set of *positive edges*, and

$$E^- = \{e \in E \mid \mu(e) \in X^-\}.$$

is called the set of *negative edges*. Clearly,  $(E^+)^{-1} = E^-$  and  $(E^-)^{-1} = E^+$ .

The *rank*  $r(\Gamma)$  of an inverse  $X$ -digraph  $\Gamma$  is defined as  $|E^+| - |T|$ , where  $T$  is any spanning subtree of  $\Gamma$ . The fundamental group  $\pi_1(\Gamma)$  is the group of labels of all cycles at the root; it is naturally a subgroup of  $F(X)$  of the rank  $r(\Gamma)$ , see [5].

### 3. PRELIMINARIES: COMPUTATIONAL MODEL AND DATA REPRESENTATION

All computations are assumed to be performed on a random access machine. We use base 2 positional number system in which presentations of integers are converted into integers via the rule:

$$(a_{k-1} \dots a_3 a_2 a_1 a_0)_2 = a_{k-1} 2^{k-1} + \dots + a_2 2^2 + a_1 2 + a_0,$$

where we assume that  $a_{k-1} = 1$ . The number  $k$  is called the *bit-length* of the presentation.

Let  $G$  be a group generated by a finite set  $X = \{x_1, \dots, x_n\}$ . We formally encode the word problem for  $G$  as a subset of  $\{0, 1\}^*$  as follows. We first encode elements of the set  $X^\pm = \{x_1^\pm, \dots, x_n^\pm\}$  by unique bit-strings of length  $\lceil \log_2 n \rceil + 1$ . The code for a word  $w = w(X_r^\pm)$  is a concatenation of codes for letters and, formally:

$$\mathbf{WP}(F/N) = \{\text{code}(w) \mid w \in N\}.$$

Thus, the bit-length of the representation for a word  $w \in F$  is:

$$|\text{code}(w)| = |w|(\lceil \log_2 n \rceil + 1).$$

We encode the power and conjugacy problems in a similar fashion. For both of these problems instances are pairs of words and the encoding can be done by introducing a new letter “,” into the alphabet  $X^\pm$ .

**3.1. Quasi-linear time complexity.** An algorithm is said to run in *quasi-linear time* if its time complexity function is  $O(n \log^k n)$  for some constant  $k \in \mathbb{N}$ . We use notation  $\tilde{O}(n)$  to denote quasi-linear time complexity. Quasi-linear time algorithms are also  $o(n^{1+\varepsilon})$  for every  $\varepsilon > 0$ , and thus run faster than any polynomial in  $n$  with exponent strictly greater than 1. See [13] for more information on quasi-linear time complexity theory. Similarly, one can define quasi-quadratic  $\tilde{O}(n^2)$ , quasi-cubic  $\tilde{O}(n^3)$  time complexity as  $O(n^2 \log^k n)$ ,  $O(n^3 \log^k n)$ , etc.

#### 4. FLOWS ON INVERSE $X$ -DIGRAPHS

Let  $\Gamma = (V, E)$  be an inverse  $X$ -digraph. We say that a function  $f : E \rightarrow \mathbb{Z}$  is *balanced* if:

(F1)  $f(e) = -f(e^{-1})$  for any  $e \in E$ .

All functions in this paper are balanced. A function  $f : E \rightarrow \mathbb{Z}$  defines the function  $\mathcal{N}_f : V \rightarrow \mathbb{Z}$ :

$$\mathcal{N}_f(v) = \sum_{\alpha(e)=v} f(e),$$

called the *net-flow* function of  $f$ . We say that  $f$  is a *flow* if it satisfies the conditions (F1), (F2), and (F3).

(F2)  $f$  has a finite support  $\text{supp}(f) = \{e \in E \mid f(e) \neq 0\}$ .

(F3) Either  $\mathcal{N}_f(v) = 0$  for every  $v \in V$  in which case we say that  $f$  is a *circulation*, or there exist  $s, t \in V$  such that  $\mathcal{N}_f(v) = 0$  for all  $v \in V \setminus \{s, t\}$ , and  $\mathcal{N}_f(s) = 1$  and  $\mathcal{N}_f(t) = -1$  and we say that  $f$  is a flow from the *source*  $s$  to the *sink*  $t$ .

Define  $\mathcal{F}_\Gamma$  to be the set of all balanced integral functions on  $E$  with finite support:

$$\mathcal{F}_\Gamma = \{f : E \rightarrow \mathbb{Z}\}.$$

For  $f, g \in \mathcal{F}_\Gamma$  define  $f + g \in \mathcal{F}_\Gamma$  as follows:

$$(f + g)(e) = f(e) + g(e).$$

Clearly,  $(\mathcal{F}_\Gamma, +)$  is an abelian group. The function  $\|\cdot\| : \mathcal{F}_\Gamma \rightarrow \mathbb{Z}$  defined by:

$$\|\pi\| = \sum_{e \in E^+} |\pi(e)|$$

is called a *norm* on  $\mathcal{F}_\Gamma$ . It is easy to see that every  $X$ -digraph morphism  $\varphi : \Gamma \rightarrow \Delta$  induces a homomorphism of abelian groups  $\rho_\varphi : \mathcal{F}_\Gamma \rightarrow \mathcal{F}_\Delta$  defined as follows:

$$\rho_\varphi(f)(e') = \sum_{\varphi(e)=e'} f(e),$$

for  $f \in \mathcal{F}_\Gamma$  and  $e' \in E(\Delta)$ . Clearly,  $\|\pi\| \geq \|\rho_\varphi(\pi)\|$  for every  $\pi \in \mathcal{F}_\Gamma$ .

**4.1. Flows defined by words.** Let  $\Gamma = (V, E)$  be an rooted folded complete inverse  $X$ -digraph and  $w = x_{i_1}^{\varepsilon_1} \dots x_{i_k}^{\varepsilon_k} \in F(X)$ . The word  $w$  defines a unique path  $p_w$  in  $\Gamma$ :

$$v_0 \xrightarrow{x_{i_1}^{\varepsilon_1}} v_1 \xrightarrow{x_{i_2}^{\varepsilon_2}} v_2 \xrightarrow{x_{i_3}^{\varepsilon_3}} \dots \xrightarrow{x_{i_k}^{\varepsilon_k}} v_k$$

where  $v_0$  is the root of  $\Gamma$ , and a function  $\pi_w^\Gamma : E \rightarrow \mathbb{Z}$  which associates to an edge  $e$  the number of times  $e$  is traversed minus the number of times  $e^{-1}$  is traversed by  $p_w$ . It is easy to check that  $\pi_w^\Gamma$  is a flow in  $\Gamma$ . We call  $\pi_w^\Gamma$  the *flow* of  $w$  in  $\Gamma$ .

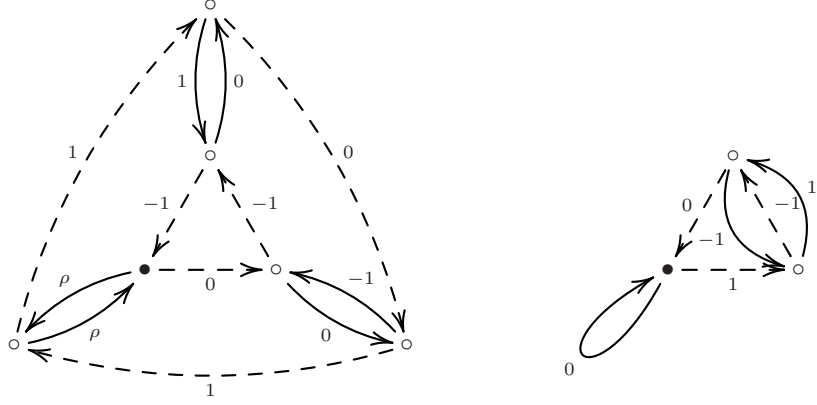


FIGURE 1. The Cayley graph of  $S_3 = \langle a, b \rangle$  with  $|a| = 3$  and  $|b| = 2$  and the Schreier graph of  $H = \langle b \rangle \leq S_3$ . The straight edges correspond to  $b$  and dashed ones to  $a$ . The values of  $\pi_w$  for  $w = [a^2, b]$  are shown on the edges.

**Lemma 4.1** (See [11, Lemma 2.5]). *For any flow  $\pi : E(\Gamma) \rightarrow \mathbb{Z}$  there exists  $w \in F(X)$  satisfying  $\pi = \pi_w^\Gamma$ .*  $\square$

In general, if  $\Gamma$  is not complete, then some words can not be traced in  $\Gamma$ . Suppose that a reduced nontrivial word  $w$  can be traced in  $\Gamma$ . The set of edges traversed by  $w$  in  $\Gamma$  forms a connected  $X$ -digraph called the *support graph* of  $w$  in  $\Gamma$ .

**Lemma 4.2.** *Let  $\Gamma$  be a rooted folded inverse  $X$ -digraph and  $m$  the length of a shortest cycle in  $\Gamma$  (not necessarily at the root). Suppose that a reduced nontrivial word  $w$  can be traced in  $\Gamma$  and  $\pi_w^\Gamma = 0$ . Then  $|w| \geq 3m$ .*

*Proof.* It follows from our assumption  $\pi_w = 0$  that the path  $p_w$  is a cycle in  $\Gamma$ . Let  $\Delta$  be the support graph of  $w$  in  $\Gamma$ . The rank of  $\Delta$  can not be 0 ( $w$  is not reduced in this case) and can not be 1 (either  $w$  is not reduced or  $\pi_w \neq 0$ ). Therefore, the rank of  $\Delta$  is at least 2. Each edge of  $\Delta$  is traversed by  $w$  at least twice. Hence, it is sufficient to prove that  $2|E(\Delta)| \geq 3m$ . Let  $\Delta'$  be a minimal subgraph of  $\Delta$  of rank exactly 2. There are exactly two distinct configurations possible for  $\Delta'$ , shown in Figure 2.

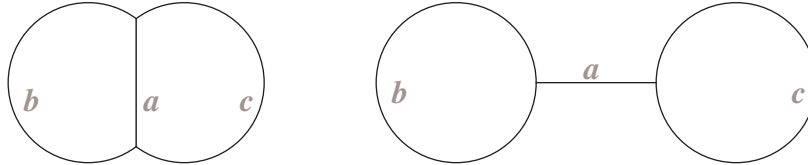


FIGURE 2. Two configurations for support graphs in Lemma 4.2.

Let  $a, b, c$  be the lengths of arcs as shown in the figure. Since, the length of a shortest cycle in  $\Gamma$  is  $m$ , we get the following bounds for our cases:

$$\begin{cases} a + b \geq m, \\ a + c \geq m, \\ b + c \geq m, \end{cases} \quad \begin{cases} b \geq m, \\ c \geq m. \end{cases}$$

In both cases we have  $2(a + b + c) \geq 3m$  which proves that  $2|E(\Delta)| \geq 3m$ . Thus,  $|w| \geq 3m$ .  $\square$

**4.2. Flows on Schreier graphs.** In this section we study properties of flows on Schreier graphs. The following lemma is the most important tool in the study of groups of the type  $F/N'$  and is the foundation of the Magnus embedding discussed in Section 5. It is a well-known result and can be proven using algebraic topology techniques. Here we provide a proof using elementary properties of Stallings' graphs.

**Lemma 4.3.** *Let  $H \leq F$ ,  $\Delta = \mathbf{Sch}(X; H)$ , and  $w \in F$ . Then  $\pi_w^\Delta = 0$  if and only if  $w \in [H, H]$ .*

*Proof.* “ $\Leftarrow$ ” If  $w \in [H, H]$ , then  $\pi_w = 0$ .

“ $\Rightarrow$ ” Assume that  $\pi_w^\Delta = 0$ . Then  $w \in H$ . Taking a spanning tree in  $\mathbf{Sch}(X; H)$  we can choose a good (perhaps infinite) set of generators  $Y$  for  $H$  corresponding to the cycles defined by positive edges outside of the spanning tree. The word  $w$  can be (uniquely) expressed as a word  $w = u(Y)$  in the generators  $Y$ . Since  $\pi_w^\Delta = 0$  we should have  $\sigma_y(u) = 0$  (algebraic sum of powers of  $y$ 's in the expression for  $u$  is 0) for every  $y \in Y$ . This means that  $u$  can be expressed as a product of commutators of elements from  $\langle Y \rangle = H$ . Hence  $w \in [H, H]$ .  $\square$

**Corollary 4.4.**  $w = 1$  in  $F/N'$  if and only if  $\pi_w^\Gamma = 0$  where  $\Gamma = \mathbf{Cay}(X; N)$ .  $\square$

**Corollary 4.5.** Let  $H \leq F$  and  $m$  is the length of a shortest nonempty word in  $H$ . Then the length of a shortest nonempty word in  $[H, H]$  is at least  $3m$ .

*Proof.* By Lemma 4.3 if  $w \in [H, H] \setminus \{\varepsilon\}$ , then  $\pi_w^\Delta = 0$  in  $\Delta = \mathbf{Sch}(X; H)$ . By Lemma 4.2,  $|w| \geq 3m$ .  $\square$

**Lemma 4.6.** *Let  $N \trianglelefteq F$ ,  $w \in F$ , and  $\Delta = \mathbf{Sch}(X; \langle N, w \rangle)$ . If  $\pi_w^\Delta = 0$ , then  $w \in N$ .*

*Proof.* If  $\pi_w^\Delta = 0$  then, by Lemma 4.3,  $w \in [\langle N, w \rangle, \langle N, w \rangle]$ . Hence,  $w$  can be expressed as a product of commutators over  $\langle N, w \rangle$ . That expresses  $w$  as a product of elements from  $N$  and  $w$ 's with the trivial algebraic sum of powers for  $w$ . That product belongs to  $N$  because  $N$  is normal in  $F$ .  $\square$

**Corollary 4.7.** Let  $N \trianglelefteq F$ ,  $w \in F \setminus N$ , and  $\Delta = \mathbf{Sch}(X; \langle N, w \rangle)$ . Then  $\pi_w^\Delta \neq 0$ .

**4.3. Flows on Cayley graphs.** Let  $X = \{x_1, \dots, x_n\}$ ,  $F = F(X)$ ,  $N \trianglelefteq F$ ,  $G = F/N$ , and  $\Gamma = \mathbf{Cay}(X; N)$ . The group  $G$  acts on its Cayley graph  $\Gamma$  by shifts:

$$e^g = g^{-1}h \xrightarrow{x} g^{-1}hx.$$

for  $g \in G$  and  $e = h \xrightarrow{x} hx \in E$ . The following action of  $\mathbb{Z}G$  on  $\mathcal{F}_\Gamma$  turns the later into a  $\mathbb{Z}G$ -module. For  $c_1g_1 + \dots + c_kg_k \in \mathbb{Z}G$  and  $f \in \mathcal{F}_\Gamma$  define  $f' = (c_1g_1 + \dots + c_kg_k)f$  on  $e = g \xrightarrow{x} gx$  to be:

$$f'(e) = c_1f(e^{g_1}) + \dots + c_kf(e^{g_k}).$$

Denote  $\pi_{x_i}$  by  $\pi_i$  for  $i = 1, \dots, n$ . The next lemma is straightforward.

**Lemma 4.8.**  $\mathcal{F}_\Gamma$  is a free  $\mathbb{Z}G$ -module of rank  $n$  with a free basis  $\{\pi_1, \dots, \pi_n\}$ . In particular, every  $\pi \in \mathcal{F}_\Gamma$  can be uniquely expressed as a  $\mathbb{Z}G$  linear combination of  $\pi_1, \dots, \pi_n$ .  $\square$

The set of circulation  $\mathcal{C}_\Gamma$  in  $\mathcal{F}_\Gamma$  is closed under addition and the scalar  $\mathbb{Z}G$ -multiplication and hence  $\mathcal{C}_\Gamma$  is a  $\mathbb{Z}G$ -submodule of  $\mathcal{F}_\Gamma$ .

**Lemma 4.9.** If  $G$  is finitely presented, then  $\mathcal{C}_\Gamma$  is a finitely generated  $\mathbb{Z}G$ -module.

*Proof.* If  $N = \mathbf{ncl}_F(r_1, \dots, r_k)$ , then  $\mathcal{C}_\Gamma = \langle \pi_{r_1}, \dots, \pi_{r_k} \rangle$ .  $\square$

There exists an algebraic way to define the net-flow function of  $\pi \in \mathcal{F}_\Gamma$ . Define a map  $\mathcal{N} : \mathcal{F}_\Gamma \rightarrow \mathbb{Z}G$  by:

$$\pi = \alpha_1 \pi_1 + \dots + \alpha_n \pi_n \xrightarrow{\mathcal{N}} \sum_{i=1}^n \alpha_i (1 - \bar{x}_i).$$

If  $\pi = \sum_{i=1}^n \sum_{g \in G} a_{g,i} g \pi_i$ , then the coefficient for  $g$  in  $\mathcal{N}(\pi)$  is

$$a_{g,1} + \dots + a_{g,n} - a_{g\gamma(x_1)^{-1},1} - \dots - a_{g\gamma(x_n)^{-1},n}$$

which is exactly the value of the net flow at  $g$  defined by  $\pi$ . Hence,  $\mathcal{N}(\pi)$  is a description of  $\mathcal{N}_\pi$  as an element of  $\mathbb{Z}G$ . The next propositions are obvious.

**Proposition 4.10.**  $\mathcal{N} : \mathcal{F}_\Gamma \rightarrow \mathbb{Z}G$  is a  $\mathbb{Z}G$ -module homomorphism.  $\square$

**Proposition 4.11.** For any  $\pi \in \mathcal{F}_\Gamma$  the following holds.

- (a)  $\pi \in \mathcal{C}_\Gamma$  if and only if  $\mathcal{N}(\pi) = 0$ .
- (b)  $\pi$  is a flow on  $\Gamma$  if and only if  $\mathcal{N}(\pi) = 1 - g$  for some  $g \in G$ .  $\square$

Consider the *augmentation map*  $\epsilon : \mathbb{Z}G \rightarrow \mathbb{Z}$ , defined by:

$$\sum_{g \in G} \alpha_g g \xrightarrow{\epsilon} \sum_{g \in G} \alpha_g.$$

Recall that  $\epsilon$  is a ring homomorphism and therefore a homomorphism of  $\mathbb{Z}G$ -modules once  $\mathbb{Z}$  is assumed to be a  $\mathbb{Z}G$ -module with trivial  $G$  action.

**Lemma 4.12.** The sequence  $\mathcal{F}_\Gamma \xrightarrow{\mathcal{N}} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z}$  is an exact sequence of  $\mathbb{Z}G$ -modules.

*Proof.* The inclusion  $\mathbf{im}(\mathcal{N}) \subseteq \ker(\epsilon)$  can be easily shown by induction on  $\|\pi\|$ . To show the opposite inclusion pick an arbitrary  $\sum \alpha_g g \in \ker(\epsilon)$ . Then

$$\sum \alpha_g g = \sum \alpha_g g - \sum \alpha_g = \sum \alpha_g (g - 1).$$

If  $G \ni g = x_{i_1}^{\epsilon_1} \dots x_{i_k}^{\epsilon_k}$ , then  $g - 1$  can be written as follows:

$$\begin{aligned} & (x_{i_1}^{\epsilon_1} \dots x_{i_k}^{\epsilon_k} - x_{i_1}^{\epsilon_1} \dots x_{i_{k-1}}^{\epsilon_{k-1}}) + (x_{i_1}^{\epsilon_1} \dots x_{i_{k-1}}^{\epsilon_{k-1}} - x_{i_1}^{\epsilon_1} \dots x_{i_{k-2}}^{\epsilon_{k-2}}) + \dots + (x_{i_1}^{\epsilon_1} - 1) \\ &= \sum_{j=0}^{k-1} x_{i_1}^{\epsilon_1} \dots x_{i_j}^{\epsilon_j} (x_{i_{j+1}}^{\epsilon_{j+1}} - 1). \end{aligned}$$

Therefore,  $-\sum \alpha_g g = \sum \alpha_g (1 - g)$  is a linear  $\mathbb{Z}G$ -combination of the elements of the form  $(1 - \bar{x}_i)$  and hence belongs to  $\mathbf{im}(\mathcal{N})$ . Thus,  $\sum \alpha_g g \in \mathbf{im}(\mathcal{N})$ .  $\square$



## 5. MAGNUS EMBEDDING

Let  $X = \{x_1, \dots, x_n\}$ ,  $F = F(X)$ ,  $N \trianglelefteq F$ , and  $\Gamma = \mathbf{Cay}(X; N)$ . In this section we study relations between groups  $G = F/N$  and  $F/N'$ . It is easy to check that the set of matrices:

$$M(X; N) = \left\{ \begin{pmatrix} g & \pi \\ 0 & 1 \end{pmatrix} \mid g \in G, \pi \in \mathcal{F}_\Gamma \right\}$$

forms a group with respect to the matrix multiplication which can be easily recognized as the wreath product  $\mathbb{Z}^n \mathbf{wr} G$ .

Let  $\bar{\cdot} : F \rightarrow F/N$  be the canonical epimorphism. Define a homomorphism  $\mu : F \rightarrow M(X; N)$  by:

$$(1) \quad x_i \xrightarrow{\mu} \begin{pmatrix} \bar{x}_i & \pi_i \\ 0 & 1 \end{pmatrix}, \quad x_i^{-1} \xrightarrow{\mu} \begin{pmatrix} \bar{x}_i^{-1} & -\bar{x}_i^{-1}\pi_i \\ 0 & 1 \end{pmatrix}.$$

It is easy to check by induction on  $|w|$  that:

$$(2) \quad \mu(w) = \begin{pmatrix} \bar{w} & \pi_w \\ 0 & 1 \end{pmatrix}.$$

**Proposition 5.1.** For any  $w \in F$  if  $\pi_w^\Gamma = 0$  then  $\bar{w} = 1$ .

*Proof.* Assume that  $\bar{w} \neq 1$  in  $F/N$ . Tracing  $w$  in  $\Gamma$  we obtain a path  $p_w$  from 1 to  $wN \neq 1$ . The path  $p_w$  is not a circuit and the corresponding flow is not a circulation, i.e.

$$\mathcal{N}_{\pi_w}(1) = \sum_{\alpha(e)=1} \pi_w^\Gamma(e) = 1.$$

Therefore,  $\pi_w^\Gamma(e) \neq 0$  for some edge  $e$  adjacent to 1. Thus,  $\pi_w^\Gamma \neq 0$ . □

Now note that for every  $w \in F$ :

$$\begin{aligned} w \in \ker(\varphi) &\Leftrightarrow \pi_w^\Gamma = 0 \text{ and } \bar{w} = 1 \\ &\Leftrightarrow \pi_w^\Gamma = 0 \text{ (by Proposition 5.1)} \\ &\Leftrightarrow w \in N' \text{ (by Lemma 4.3),} \end{aligned}$$

which proves the following theorem.

**Theorem 5.2** (See [7]). Let  $F = F(x_1, \dots, x_n)$ ,  $N \trianglelefteq F$ , and  $\bar{\cdot} : F \rightarrow F/N$  be the canonical epimorphism. The homomorphism  $\mu : F \rightarrow M(X; N)$  defined by

$$x \xrightarrow{\mu} \begin{pmatrix} \bar{x} & \pi_x \\ 0 & 1 \end{pmatrix}$$

satisfies  $\ker(\mu) = N'$ . Therefore,  $F/N' \simeq \mu(F) \leq M(X; N)$ . The induced embedding  $F/N' \rightarrow M(X; N)$  is called the Magnus embedding. □

**5.1. Properties of Magnus embedding.** The following proposition was proved in [15] using Fox derivatives. Let  $g \in G$ ,  $\pi = \sum_{i=1}^n \alpha_i \pi_i \in \mathcal{F}_\Gamma$ , and

$$A = \begin{pmatrix} g & \sum_{i=1}^n \alpha_i \pi_i \\ 0 & 1 \end{pmatrix}.$$

**Proposition 5.3** (See [15, Theorem 2]). The following holds.

- (a)  $A \in \mu(F)$  if and only if  $\sum_{i=1}^n \alpha_i (1 - \bar{x}_i) = 1 - g$ .
- (b)  $A \in \mu(N)$  if and only if  $\sum_{i=1}^n \alpha_i (1 - \bar{x}_i) = 0$ .

*Proof.* Follows from (2) and Proposition 4.11.  $\square$

For a nontrivial  $g \in G$  define a map  $\tau_g : \mathcal{F}_\Gamma \rightarrow \mathcal{F}_\Gamma$  by:

$$\pi \xrightarrow{\tau_g} (1 - g)\pi.$$

Denote  $\mathbf{Sch}(X; \langle N, g \rangle)$  by  $\Delta$ . The natural projection  $\varphi : \Gamma \rightarrow \Delta$  induces an abelian group homomorphism  $\rho_g : \mathcal{F}_\Gamma \rightarrow \mathcal{F}_\Delta$ . Properties of the functions  $\tau_g$  and  $\rho_g$  are very important in the study of the conjugacy problem in  $F/N'$ .

**Lemma 5.4.** *The sequence  $\mathcal{F}_\Gamma \xrightarrow{\tau_g} \mathcal{F}_\Gamma \xrightarrow{\rho_g} \mathcal{F}_\Delta$  is an exact sequence of abelian groups.*

*Proof.* The image of  $\tau_g$  is a subgroup of  $\mathcal{F}_\Gamma$  generated by the elements  $(1 - g)h\pi_i$  for  $h \in G$  and  $i = 1, \dots, n$ . Clearly,  $\rho_g((1 - g)h\pi_i) = 0$ .

Conversely, assume that  $\pi' = \rho_g(\pi) = 0$ . Let  $H = \langle N, g \rangle$ . Consider any edge  $e' = Hh \xrightarrow{x_i} Hhx_i$  in  $\Delta$ . By definition of  $\rho_g$  we get

$$0 = \pi'(e') = \sum_{\varphi(e)=e'} \pi(e) = \sum_{g^j} \pi(Ng^j h \xrightarrow{x_i} Ng^j hx_i),$$

where  $g^j$  ranges over all distinct powers of  $g$ . It is easy to see that such  $\pi$  is an integral linear combination of the elements  $(1 - g)h\pi_i$  and, hence, belongs to  $\mathbf{im}(\tau_g)$ .  $\square$

**Lemma 5.5** (Cf. [4, Lemma 4]).  *$\ker(\tau_g)$  is not trivial if and only if  $|g| = k < \infty$ , in which case it is an abelian subgroup of  $\mathcal{F}_\Gamma$ :*

$$\ker(\tau_g) = \langle (1 + g + \dots + g^{k-1})h\pi_i \mid h \in G \text{ and } i = 1, \dots, n \rangle.$$

*Proof.* Pick any  $\pi \in \mathcal{F}_\Gamma$  such that  $(1 - g)\pi = 0$ . Then  $g^j\pi = \pi$  for every  $j \in \mathbb{Z}$ , which can not happen if  $|g| = \infty$  since  $\pi$  has finite support. Assume that  $|g| = k < \infty$ . It is straightforward to check that  $(1 + g + \dots + g^{k-1})h\pi_i \in \ker(\tau_g)$ . On the other hand if  $g^j\pi = \pi$  for every  $j \in \mathbb{Z}$ , then the coefficients  $\alpha_{h,i}$  are constant on right  $\langle g \rangle$ -cosets and hence are linear combinations of the generators.  $\square$

**Lemma 5.6.** *Let  $\pi \in \mathcal{F}_\Gamma$  and  $1 \neq g \in G$ . If  $(1 - g)\pi \in \mathcal{C}_\Gamma$ , then there exists  $\pi^* \in \mathcal{C}_\Gamma$  satisfying  $(1 - g)\pi = (1 - g)\pi^*$ .*

*Proof.* If  $(1 - g)\pi \in \mathcal{C}_\Gamma$ , then

$$\mathcal{N}((1 - g)\pi) = \mathcal{N}(\pi) - g\mathcal{N}(\pi) = 0.$$

Therefore,  $\mathcal{N}(\pi) = g^j\mathcal{N}(\pi)$  for every  $j \in \mathbb{Z}$ .

CASE-I. Assume that  $|g| = \infty$ . Since  $\mathcal{N}(\pi)$  has finite support, it must be the case that  $\mathcal{N}(\pi) = 0$ . Thus,  $\pi \in \mathcal{C}_\Gamma$ .

CASE-II. Assume that  $|g| = k < \infty$ . Then:

$$\mathcal{N}(\pi) = g\mathcal{N}(\pi) = \dots = g^{k-1}\mathcal{N}(\pi),$$

i.e.,  $\mathcal{N}(\pi)$  is constant on right  $\langle g \rangle$ -cosets. Hence,

$$\mathcal{N}(\pi) = (1 + g + \dots + g^{k-1})N', \quad \text{for some } N' \in \mathbb{Z}G.$$

By Lemma 4.12, we have:

$$0 = \epsilon(\mathcal{N}(\pi)) = \epsilon(1 + g + \dots + g^{k-1})\epsilon(N') = k\epsilon(N') \quad \text{in } \mathbb{Z},$$

which implies that  $\epsilon(N') = 0$ . Hence  $N' \in \ker(\epsilon)$  and by Lemma 4.12:

$$N' = \sum \alpha_i(1 - \bar{x}_i) \quad \text{for some } \alpha_i \in \mathbb{Z}G.$$

Put  $\pi' = \alpha_1\pi_1 + \dots + \alpha_n\pi_n \in \mathcal{F}_\Gamma$ . Notice that  $N' = \mathcal{N}(\pi')$  and:

$$\mathcal{N}(\pi) = (1 + g + \dots + g^{k-1})\mathcal{N}(\pi').$$

Define  $\pi^* = \pi - (1 + g + \dots + g^{k-1})\pi'$  and observe that:

$$\mathcal{N}(\pi^*) = 0 \text{ and } (1 - g)\pi = (1 - g)\pi^*,$$

i.e.,  $\pi^*$  is a required element.  $\square$

## 6. ALGORITHMIC PROPERTIES OF GROUPS $F/N^{(d)}$

In this section we study relations between algorithmic problems in groups  $\{F/N^{(d)}\}_{d=0}^\infty$ , where  $N^{(d)}$  denotes the  $d$ th derived subgroup of  $N$ .

**6.1. Word problem.** Here we review the relations between the word problems in groups  $\{F/N^{(d)}\}$ .

**Proposition 6.1.**  $\mathbf{WP}(F/N) \Rightarrow \mathbf{WP}(F/N')$ .

*Proof.* Let  $\Gamma = \mathbf{Cay}(X; N)$ . By Lemma 4.3,  $w = x_{i_1}^{\varepsilon_1} \dots x_{i_k}^{\varepsilon_k}$  represents the identity in  $F/N'$  if and only if  $\pi_w^\Gamma = 0$ . To describe the function  $\pi_w^\Gamma$  one needs to distinguish edges in  $\Gamma$  traversed by  $w$ :

$$\varepsilon \xrightarrow{x_{i_1}^{\varepsilon_1}} w_1 \xrightarrow{x_{i_2}^{\varepsilon_2}} w_2 \xrightarrow{x_{i_2}^{\varepsilon_2}} \dots \xrightarrow{x_{i_k}^{\varepsilon_k}} x_{i_1}^{\varepsilon_1} \dots x_{i_k}^{\varepsilon_k},$$

which can be done because by assumption  $\mathbf{WP}(F/N)$  is decidable.  $\square$

**Proposition 6.2.** Let  $w \in F \setminus \{\varepsilon\}$ . If  $w = 1$  in  $F/N^{(d)}$ , then  $|w| \geq 3^d$ .

*Proof.* Easy induction on  $d$  using Lemma 4.2.  $\square$

**Corollary 6.3.** For any  $N \trianglelefteq F$  the sequence of groups  $F/N^{(d)}$  converges to  $F$  in Gromov-Hausdorff topology.  $\square$

**Theorem 6.4.** If  $\mathbf{WP}(F/N) \in \tilde{O}(T(n))$ , then  $\mathbf{WP}(F/N') \in \tilde{O}(T(n)n^2)$ . Furthermore,  $\mathbf{WP}(F/N^{(d)}) \in \tilde{O}(T(n)n^2)$  for every  $d \in \mathbb{N}$ .

*Proof.* It requires  $|w|^2$  calls of the  $\mathbf{WP}(F/N)$  to construct the support graph for a given word  $w$ . Given the support graph for  $w$  it is straightforward to construct the flow for  $w$  in  $\mathbf{Cay}(F/N)$  as described in [18, Section 2]. By Proposition 6.2, to solve  $\mathbf{WP}(F/N^{(d)})$  one must iterate the procedure at most  $\log_3 |w|$  times.  $\square$

The converse to Proposition 6.1 also holds. It was first proven in [1] using Bronstein monotonicity theorem. Here we use Auslander-Lyndon theorem which gives the most straightforward algorithm.

**Theorem 6.5.** Assume that  $N$  is a recursively enumerable normal subgroup of  $F$  and  $N'$  is recursive, then  $N$  is recursive.

*Proof.* The statement is obvious for abelian  $F$  or  $N = \{1\}$ . Assume that  $F$  is not abelian and  $N$  is not trivial. Then  $N$  has rank at least 2. By [2, Theorem 1], for any  $v \in F \setminus N$  there exists  $w \in N$  such that  $[v, w] \notin N'$ . That gives a procedure for testing if  $v \notin N$ . Thus,  $N$  is recursive.  $\square$

**Corollary 6.6.** Assume that  $N$  is a recursively enumerable normal subgroup of  $F$  and  $\mathbf{WP}(F/N^{(d)})$  is decidable for some  $d \in \mathbb{N}$ . Then  $\mathbf{WP}(F/N^{(d)})$  is decidable for every  $d \in \mathbb{N}$ .  $\square$

**6.2. Power problem.** In this section we use properties of Magnus embedding to prove that the group  $F/N'$  is torsion free and to solve the power problem in  $F/N'$ . Let  $\Gamma = \mathbf{Cay}(X; N)$ .

**Lemma 6.7.** *For every  $w \notin N'$  and  $k \in \mathbb{N}$  we have  $\|\pi_{w^k}^\Gamma\| \geq k$ .*

*Proof.* Assume that  $w \notin N'$  and consider two cases.

CASE-I: If  $w \in N$ , then  $\|\pi_w^\Gamma\| \geq 1$  and  $\|\pi_{w^k}^\Gamma\| = \|k\pi_w^\Gamma\| \geq k$  for every  $k \in \mathbb{N}$ .

CASE-II: Assume that  $w \notin N$  and denote  $\mathbf{Sch}(X; \langle N, w \rangle)$  by  $\Delta$ . By Lemma 4.6,  $\|\pi_w^\Delta\| \geq 1$  and  $\|\pi_{w^k}^\Delta\| = \|k\pi_w^\Delta\| \geq k$  for every  $k \in \mathbb{N}$ . The later implies that  $\|\pi_{w^k}^\Gamma\| \geq k$ .  $\square$

**Theorem 6.8.** *For every  $N \trianglelefteq F$  the group  $F/N'$  is torsion free.*

*Proof.* By Lemma 6.7, if  $w \notin N'$  and  $k \in \mathbb{N}$ , then  $\|\pi_{w^k}^\Gamma\| \geq k$ , i.e.,  $w^k \notin N'$ .  $\square$

**Lemma 6.9.** *Let  $u, v \in F$  and  $u \notin N'$ . If  $u^k = v$  in  $F/N'$ , then  $k \leq |v|$ .*

*Proof.* If  $|v| < k$ , then  $\|\pi_v\| < k \leq \|\pi_{u^k}\|$ , which means that  $u^k \neq v$  in  $F/N'$ .  $\square$

**Theorem 6.10.** *If  $\mathbf{WP}(F/N)$  is decidable, then  $\mathbf{PP}(F/N')$  is decidable. Furthermore, if  $\mathbf{WP}(F/N) \in \tilde{O}(T(n))$ , then  $\mathbf{PP}(F/N^{(d)}) \in \tilde{O}(T(L^2)L)$  for every  $d \in \mathbb{N}$ , where  $L = |u| + |v|$  is the size of the input.*

*Proof.* By Lemma 6.9, given  $u, v \in F$  it is sufficient to check if  $v = u^k$  in  $F/N'$  for  $k = -|v|, \dots, |v|$  which reduces to  $2|v| + 1 = O(L)$  calls of the word problem in  $F/N'$  for words  $v^{-1}u^{-|v|}, \dots, v^{-1}u^{|v|}$  whose lengths are bounded by  $|v| + |u| \cdot |v| = O(L^2)$ .  $\square$

**6.3. Conjugacy problem.** Matthews proved in [8, Theorem B] that:

$$\mathbf{CP}(M(X; N)) \Leftrightarrow \begin{cases} \mathbf{CP}(F/N), \\ \mathbf{PP}(F/N). \end{cases}$$

The main result of this section states that restricting the conjugacy problem from  $M(X; N)$  to  $F/N'$  gives a problem equivalent to  $\mathbf{PP}(F/N)$ . In general, decidability of  $\mathbf{CP}(F/N)$  is irrelevant to decidability of  $\mathbf{CP}(F/N')$ .

The theorem below was first proved by Remeslennikov and Sokolov in [15] for a torsion free group  $F/N$  and by C. Gupta in [4] for any finitely generated group  $F/N$ .

**Theorem 6.11.** *For any  $u, v \in F$  the matrices*

$$\mu(u) = \begin{pmatrix} \bar{u} & \pi_u^\Gamma \\ 0 & 1 \end{pmatrix} \text{ and } \mu(v) = \begin{pmatrix} \bar{v} & \pi_v^\Gamma \\ 0 & 1 \end{pmatrix}$$

*are conjugate in  $M(X; N)$  if and only if they are conjugate in  $\mu(F)$ .*

*Proof.* Assume that for some  $c \in F$  and  $\pi \in \mathcal{F}_\Gamma$  the matrix

$$(3) \quad w = \begin{pmatrix} \bar{c} & \pi \\ 0 & 1 \end{pmatrix} \in M$$

conjugates  $\mu(u)$  into  $\mu(v)$ . Then  $\bar{c}^{-1}\bar{u}\bar{c} = \bar{v}$ .

CASE-I. If  $\bar{u} = \bar{v} = 1$  in  $F/N$ , then it is easy to check that the matrix

$$\begin{pmatrix} \bar{c} & \pi_c^\Gamma \\ 0 & 1 \end{pmatrix} \in \mu(F)$$

is a conjugator for  $\mu(u)$  and  $\mu(v)$  as well.

CASE-II. Assume that  $\bar{u}, \bar{v} \neq 1$  in  $F/N$ . Conjugating  $\mu(u)$  by  $\mu(c)$  we obtain an equivalent instance of the conjugacy problem with the conjugator (3) having trivial upper-left entry. Hence, from the beginning we may assume that the  $\bar{c} = 1$  and  $\bar{u} = \bar{v}$ . That gives the equality:

$$\begin{pmatrix} 1 & -\pi \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{u} & \pi_u^\Gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \pi \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{v} & \pi_v^\Gamma \\ 0 & 1 \end{pmatrix}$$

which implies that  $\pi_u^\Gamma - \pi_v^\Gamma = (1 - \bar{u})\pi$ . Since  $\pi_u^\Gamma - \pi_v^\Gamma \in \mathcal{C}_\Gamma$ , by Lemma 5.6, there exists a circulation  $\pi^*$  satisfying  $\pi_u^\Gamma - \pi_v^\Gamma = (1 - \bar{u})\pi^*$ . The matrix

$$\begin{pmatrix} 1 & \pi^* \\ 0 & 1 \end{pmatrix} \in \mu(F)$$

is a required conjugator for  $\mu(u)$  and  $\mu(v)$ .  $\square$

**Theorem 6.12** (Geometry of conjugacy problem). *Let  $N \trianglelefteq F$ ,  $u, v \in F$ , and  $\Delta = \mathbf{Sch}(X, \langle N, u \rangle)$ . Then  $u \sim v$  in  $F/N'$  if and only if there exists  $c \in F$  satisfying the conditions:*

- (a)  $\pi_u^\Delta = \bar{c}\pi_v^\Delta$ , i.e.,  $\pi_u$  can be obtained by a  $\bar{c}$ -shift of  $\pi_v$  in  $\Delta$ ;
- (b)  $\bar{c}^{-1}\bar{u}\bar{c} = \bar{v}$  in  $F/N$ .

*Proof.* By Theorem 6.11,  $u \sim v$  in  $F/N'$  if and only if  $\mu(u) \sim \mu(v)$  in  $M(X; N)$ . The conjugacy equation for  $\mu(u)$  and  $\mu(v)$  is:

$$\begin{pmatrix} \bar{c}^{-1} & -\bar{c}^{-1}\pi \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{u} & \pi_u^\Gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{c} & \pi \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{v} & \pi_v^\Gamma \\ 0 & 1 \end{pmatrix}$$

for some  $c \in F$  and  $\pi \in \mathcal{F}_\Gamma$ , which is equivalent to the system:

$$(4) \quad \begin{cases} \bar{c}^{-1}\bar{u}\bar{c} = \bar{v}, \\ \pi_u^\Gamma - \bar{c}\pi_v^\Gamma = (1 - \bar{u})\pi. \end{cases}$$

By Lemma 5.4, the equality  $\pi_u^\Gamma - \bar{c}\pi_v^\Gamma = (1 - \bar{u})\pi$  holds if and only if  $\pi_u^\Delta - \bar{c}\pi_v^\Delta = 0$ .  $\square$

**Theorem 6.13.** *If  $\mathbf{PP}(F/N)$  is decidable, then  $\mathbf{CP}(F/N')$  is decidable. Furthermore, if  $\mathbf{PP}(F/N) \in \tilde{O}(T(n))$ , then  $\mathbf{CP}(F/N^{(d)}) \in \tilde{O}(T(L^2)L^4)$  for every  $d \in \mathbb{N}$ , where  $L = |u| + |v|$  is the size of the input.*

*Proof.* We may assume that  $u \neq 1$  and  $v \neq 1$  in  $F/N'$ . If  $u = 1$  in  $F/N$ , then  $\pi_u^\Delta = \pi_u^\Gamma \neq 0$ . If  $u \neq 1$  in  $F/N$ , then by Corollary 4.7, we get the same:

$$\pi_u^\Delta \neq 0.$$

It shows that Case (2) in the proof of [8, Theorem B] is impossible in  $F/N'$  and allows to drop decidability of  $\mathbf{CP}(F/N)$ . The rest of the proof is essentially the same as that of Case (3) in the proof of [8, Theorem B].

Let  $u = x_1 \dots x_s \in F$  and  $v = y_1 \dots y_t \in F$ , where  $x_i, y_j \in X^\pm$ . For  $i = 1, \dots, s$  and  $j = 1, \dots, t$  define words:

$$u_i = x_1 \dots x_i, \quad v_j = y_1 \dots y_j, \quad \text{and } c_{i,j} = u_i v_j^{-1}.$$

Fix  $i$  such that  $\pi_u^\Delta(u_{i-1} \rightarrow u_i) \neq 0$ . The set of solutions of the equation  $\pi_u = \bar{c}\pi_v$  is a finite (perhaps trivial) union of some cosets  $\langle u \rangle c_{i,j}$  in  $F/N$ . Since  $\mathbf{PP}(F/N)$  is decidable we can directly check the equalities  $\pi_u^\Delta = \bar{c}_{i,j}\pi_v^\Delta$  and  $\bar{c}_{i,j}^{-1}\bar{u}\bar{c}_{i,j} = \bar{v}$ . Hence,  $\mathbf{CP}(F/N')$  is decidable.

For every  $c_{i,j}$  the described algorithm for  $\mathbf{CP}(F/N')$  makes  $O(L^2)$  calls of the subroutine for  $\mathbf{PP}(F/N)$  with instances  $(u, c_{i,j}v_k u_l)$  of size  $O(L)$ . Hence overall complexity of testing  $\pi_u = \bar{c}\pi_v$  is  $\tilde{O}(T(L^2)L \cdot L^2 \cdot L)$ . Thus the claimed complexity bound.  $\square$

Our next goal is to prove the converse of Theorem 6.13.

**Proposition 6.14.** Let  $N \trianglelefteq F$  and  $u, v \in F \setminus N$  satisfy  $[u, v] = 1$  in  $F/N$ . Then  $v \in \langle u \rangle$  in  $F/N$  if and only if  $u \sim u[w, v]$  in  $F/N'$  for every  $w \in \langle N, u \rangle$ .

*Proof.* Let  $\Delta = \mathbf{Sch}(X; \langle N, u \rangle)$ . Since  $[u, v] = 1$  in  $F/N$ , we have  $v^{-1}\langle N, u \rangle v = \langle N, u \rangle$ , i.e.,  $v$  normalizes  $\langle N, u \rangle$ . Therefore,  $\langle N, u \rangle \trianglelefteq \langle N, u, v \rangle$  and the following holds.

$$\begin{aligned} v \in \langle u \rangle \text{ in } F/N &\Leftrightarrow v \in \langle N, u \rangle \text{ in } F \\ &\Leftrightarrow [w, v] \in \langle N, u \rangle' \leq N, \quad \forall w \in \langle N, u \rangle \quad (\text{by [2, Theorem 1]}) \\ &\Leftrightarrow \pi_{[w, v]}^\Delta = 0 \text{ and } [w, v] = 1 \text{ in } F/N, \quad \forall w \in \langle N, u \rangle \\ &\Leftrightarrow \pi_u^\Delta = \pi_{u[w, v]}^\Delta \text{ and } u = u[w, v] \text{ in } F/N, \quad \forall w \in \langle N, u \rangle. \end{aligned}$$

By Theorem 6.12 the later holds if and only if  $u \sim u[w, v]$  in  $F/N'$  for every  $w \in \langle N, u \rangle$ .  $\square$

**Theorem 6.15** (Cf. [1, Lemma 1]). Assume that  $N$  is recursively enumerable. Then  $\mathbf{CP}(F/N') \Rightarrow \mathbf{PP}(F/N)$ .

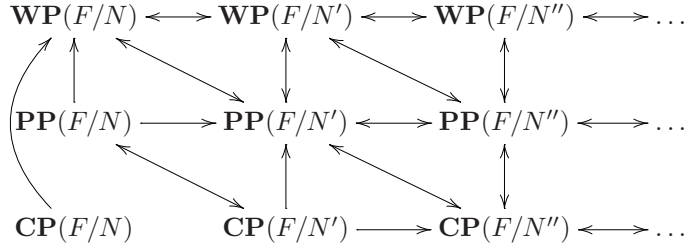
*Proof.* By assumption  $\mathbf{CP}(F/N')$  is decidable. Hence  $\mathbf{WP}(F/N')$  is decidable and  $\mathbf{WP}(F/N)$  is decidable. Consider an arbitrary instance  $u, v \in F$  of  $\mathbf{PP}(F/N)$ . Our goal is to decide if  $v \in \langle u \rangle$  in  $F/N$ , or not.

- If  $v = 1$  in  $F/N$ , then the answer is YES.
- If  $u = 1$  in  $F/N$  and  $v \neq 1$ , then the answer is NO.
- If  $[u, v] \neq 1$  in  $F/N$ , then the answer is NO.

Hence, we may assume that  $u \neq 1$ ,  $v \neq 1$ , and  $[u, v] = 1$  in  $F/N$ .

To test if  $v \in \langle u \rangle$  in  $F/N$  we run a process that checks if  $v = u^k$  in  $F/N$  for some  $k \in \mathbb{Z}$ . To test if  $v \notin \langle u \rangle$  in  $F/N$  we enumerate all words  $w \in \langle N, u \rangle$  and solve the conjugacy problem for words  $u$  and  $u[w, v]$  in  $F/N'$ . By Proposition 6.14, if  $v \notin \langle u \rangle$  then a negative instance will be found eventually.  $\square$

**6.4. Relations among the algorithmic problems.** Theorems 6.10, 6.13, and 6.15 give the following diagram of problem reducibility for a finitely generated recursively presented group  $F/N$ :



Below we deduce a few corollaries in the spirit of [9, Problem 12.98].

**Corollary 6.16.** For every recursively enumerable  $N \trianglelefteq F$  the following holds.

- (a)  $\mathbf{PP}(F/N')$  is decidable if and only if  $\mathbf{PP}(F/N'')$  is decidable.
- (b)  $\mathbf{CP}(F/N'')$  is decidable if and only if  $\mathbf{CP}(F/N''')$  is decidable.
- (c)  $\mathbf{WP}(F/N'')$  is decidable if and only if  $\mathbf{PP}(F/N'')$  is decidable if and only if  $\mathbf{CP}(F/N'')$  is decidable.  $\square$

Existence of a group  $F/N$  with decidable  $\mathbf{CP}(F/N)$  and undecidable  $\mathbf{CP}(F/N')$  was shown by Anokhin in [1] (his result is somewhat similar to Theorem 6.15, but is weaker).

**Theorem 6.17.** *There exists a recursive  $N \trianglelefteq F$  with undecidable  $\mathbf{CP}(F/N)$  and decidable  $\mathbf{CP}(F/N')$ .*

*Proof.* C. Miller introduced the following construction in [12]. Let  $U$  be a group given by a finite presentation:

$$U = \langle s_1, \dots, s_n \mid R_1, \dots, R_m \rangle.$$

Define a new group  $G(U)$  with generators  $q, s_1, \dots, s_n, t_1, \dots, t_m, d_1, \dots, d_m$  and relations of several types:

- $t_i^{-1}qt_i = qR_i$ ;
- $t_i^{-1}s_k t_i = s_k$ ;
- $d_j^{-1}qd_j = s_j^{-1}qs_j$ ;
- $d_j^{-1}s_k d_j = s_k$ ;

for all  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ , and  $1 \leq k \leq n$ . The group  $G(U)$  can be easily recognized as a multiple HNN-extension of a free group on generators  $\{q, s_1, \dots, s_n\}$  with stable letters  $t_1, \dots, t_m, d_1, \dots, d_m$ . Hence,  $\mathbf{WP}(G(U))$  is decidable (by Britton lemma) by computing reduced forms. Cyclically reduced forms are computable as well and hence  $\mathbf{PP}(G(U))$  is decidable. Miller proved in [12] that  $\mathbf{CP}(G(U))$  is decidable if and only if  $\mathbf{WP}(U)$  is decidable. Thus, choosing a finitely presented group  $U = \langle X \mid R \rangle$  with undecidable word problem we obtain a group  $G(U)$  with the required property.  $\square$

Examples of finitely presented groups  $F/N$  with solvable word problem and undecidable power problem exist (can be deduced from [14, Corollary 1]). For such groups  $\mathbf{CP}(F/N')$  is undecidable and  $\mathbf{CP}(F/N'')$  is decidable. This shows that, in general, both implications of [9, Problem 12.98(b)] fail.

**6.5. Some combinatorial problems for groups  $F/N^{(d)}$ .** In [10], the authors introduce a number of certain decision, search and optimization algorithmic problems in groups, such as *subset sum problem*, *knapsack problem*, and *bounded submonoid membership problem*. These problems are collectively referred to as *knapsack-type problems* and deal with different generalizations of the classical knapsack and subset sum problems over  $\mathbb{Z}$  to the case of arbitrary groups. Here we consider the subset sum problem and its generalization called *acyclic graph membership problem* as defined in [3].

**SSP( $G$ ), subset sum problem in  $G$ :** Given  $g_1, \dots, g_k, g \in G$  decide if

$$(5) \quad g = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k}$$

for some  $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$ .

**AGP( $G$ ), acyclic graph membership problem in  $G$ :** Given  $g \in G$  and a finite acyclic oriented graph  $\Gamma$  labeled by words in  $X^\pm$ , decide whether there is a directed path in  $\Gamma$  labeled by a word  $w$  such that  $w = g$  in  $G$ .

These problems were shown to be hard in a vast class of groups. Below we prove that they are hard in most groups of the type  $F/N^{(d)}$ .

**Theorem 6.18.** *If  $\mathbf{WP}(F/N) \in \mathbf{P}$ ,  $N \neq \{1\}$ , and  $[F : N] = \infty$ , then  $\mathbf{SSP}(F/N')$  and hence  $\mathbf{AGP}(F/N')$  are  $\mathbf{NP}$ -complete.*

*Proof.* We claim that under our assumptions the following holds.

- (a)  $N/N'$  is free abelian of infinite rank.
- (b) It requires polynomial time to find  $n$  linearly independent elements in  $N/N'$ .

Clearly, (a) and (b) allow us to reduce zero-one equation problem (ZOE) known to be  $\mathbf{NP}$ -complete to  $\mathbf{SSP}(F/N')$ .

Choose a shortest nontrivial relation  $u$  in  $F/N$ . By  $B_c$  we denote the ball of radius  $|u|$  in  $F/N$  centered at  $c$ . Put  $c_1 = 1$ . Choose  $c_2 \in F/N \setminus B_{c_1}$  and, in general, choose:

$$c_{n+1} \in F/N \setminus (B_{c_1} \cup \dots \cup B_{c_n}).$$

It is clear from the choice of  $c_i$ 's that the set of elements:

$$\{c_i u c_i^{-1} \mid i = 1, \dots, n\},$$

freely generates a free abelian group of rank  $n$  in  $F/N'$ . Furthermore, it requires polynomial time in  $n$  to construct such a set.  $\square$

**Proposition 6.19.** *If  $\mathbf{WP}(F/N) \in \mathbf{P}$  and  $[F : N] < \infty$ , then  $\mathbf{SSP}(F/N')$  is in  $\mathbf{P}$ .*

*Proof.* The condition  $[F : N] < \infty$  implies that the group  $F/N'$  is virtually abelian (of finite rank). Then by [10, Theorem 3.3],  $\mathbf{SSP}(F/N') \in \mathbf{P}$ .  $\square$

**Theorem 6.20.** *Let  $N \trianglelefteq F$ . Then  $\mathbf{SSP}(F/N') \in \mathbf{P}$  if and only if  $\mathbf{WP}(F/N) \in \mathbf{P}$  and either  $N = \{1\}$  or  $[F : N] < \infty$ .*  $\square$

**Corollary 6.21.** *Let  $N \trianglelefteq F$ . Then  $\mathbf{AGP}(F/N') \in \mathbf{P}$  if and only if  $\mathbf{WP}(F/N) \in \mathbf{P}$  and either  $N = \{1\}$  or  $[F : N] < \infty$ .*  $\square$

**Corollary 6.22.** *Let  $\{1\} \triangleleft N \trianglelefteq F$  and  $\mathbf{WP}(F/N) \in \mathbf{P}$ . Then  $\mathbf{SSP}(F/N^{(d)})$  is  $\mathbf{NP}$ -complete for every  $d \geq 2$ .*  $\square$

This gives an example of a class of groups with  $\mathbf{NP}$ -hard subset sum problem which Gromov-Hausdorff limit has subset sum problem in  $\mathbf{P}$ .

## REFERENCES

- [1] M. Anokhin. On the word problem and the conjugacy problem for groups of the form  $F/V(R)$ . *Math. Notes.*, 61(1):3–8, 1997.
- [2] M. Auslander and R. Lyndon. Commutator subgroups of free groups. *Amer. J. Math.*, 77(4):929–931, 1955.
- [3] L. Frenkel, A. Nikolaev, and A. Ushakov. Knapsack problems in products of groups. Preprint. Available at <http://arxiv.org/abs/1408.6509>, 2014.
- [4] C. Gupta. On the conjugacy problem in  $F/R'$ . *Proc. Amer. Math. Soc.*, 85(2):149–153, 1982.
- [5] I. Kapovich and A. G. Miasnikov. Stallings foldings and subgroups of free groups. *J. Algebra*, 248:608–668, 2002.
- [6] I. Lysenok and A. Ushakov. Spherical quadratic equations in free metabelian groups. to appear in Proceedings of the American Mathematical Society. Available at <http://arxiv.org/abs/1304.4898>.



- [7] W. Magnus. On a theorem of Marshall Hall. *Ann. of Math.*, 40(2):764–768, 1939.
- [8] J. Matthews. The conjugacy problem in wreath products and free metabelian groups. *Trans. Amer. Math. Soc.*, 121:329–339, 1966.
- [9] V. Mazurov and E. Khukhro. Unsolved Problems in Group Theory. The Kourovka Notebook. No. 18. Available at <http://arxiv.org/abs/1401.0300>, 2014.
- [10] A. G. Miasnikov, A. Nikolaev, and A. Ushakov. Knapsack problems in groups. To appear in *Mathematics of Computation*. Available at <http://arxiv.org/abs/1302.5671>, 2014.
- [11] A. G. Miasnikov, V. Romankov, A. Ushakov, and A. Vershik. The word and geodesic problems in free solvable groups. *Trans. Amer. Math. Soc.*, 362:4655–4682, 2010.
- [12] C. F. Miller III. *On group-theoretic decision problems and their classification*, volume 68 of *Annals of Mathematics Studies*. Princeton University Press, 1971.
- [13] A. Naik, K. Regan, and D. Sivakumar. On quasilinear-time complexity theory. *Theoret. Comput. Sci.*, 148(2):325–349, 1995.
- [14] A. Ol’shanskii and M. Sapir. Length functions on subgroups in finitely presented groups. In *Proceedings of the International Conference held at Pusan National University*, De Gruyter Proceedings in Mathematics, pages 297–304. De Gruyter, 1998.
- [15] V. N. Remeslennikov and V. G. Sokolov. Certain properties of Magnus embedding. *Algebra i Logika*, 9(5):566–578, 1970.
- [16] V. Roman’kov. Equations in free metabelian groups. *Sib. Math. J.*, 20:469–471, 1979.
- [17] J. Stallings. Topology of finite graphs. *Invent. Math.*, 71:551–565, 1983.
- [18] A. Ushakov. Algorithmic theory of free solvable groups: randomized computations. *J. Algebra*, 407:178–200, 2014.
- [19] S. Vassilieva. Polynomial time conjugacy in wreath products and free solvable groups. *Groups Complex. Cryptol.*, 3:105–120, 2011.
- [20] S. Vassilieva. The Magnus embedding is a quasi-isometry. *Int. J. Algebra Comput.*, 22:1240005, 2012.

DEPARTMENT OF MATHEMATICS, STEVENS INSTITUTE OF TECHNOLOGY, HOBOKEN, NJ, USA  
 E-mail address: msohrabi,fgul,aushakov@stevens.edu